PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-072184
(43)Date of publication of application : 04.03.2004

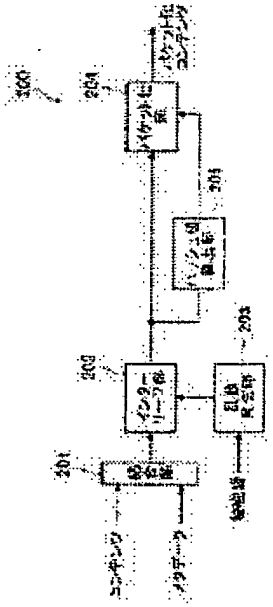
(51)Int.Cl. H04L 9/32
H04L 9/08
H04L 9/14
H04N 7/08
H04N 7/081

(21)Application number : 2002-225034
(22)Date of filing : 01.08.2002

(71)Applicant : NIPPON HOSO KYOKAI <NHK>
(72)Inventor : OGAWA KAZUTO
GOSHI SEIICHI
MUROTA ITSURO
OTAKE TAKESHI

(54) DATA TAMPERING PREVENTION APPARATUS AND PROGRAM THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a data tampering prevention apparatus capable of making the tampering of contents or metadata difficult and to provide a program therefor.
SOLUTION: The data tampering prevention apparatus is provided with: a coupling means 201 for coupling received contents and metadata to each other to produce coupled data; a random number generating means 203 for using a private key to generate a random number; an interleave means 202 for modifying a data arrangement in the couple data to produce rearrangement data; a hash value calculation means 205 for calculating a hash value in response to data of a prescribed part of the rearranged data; and a packetizing means 204 for converting the data of the prescribed part of the rearranged data in response to the hash value to produce packetized contents, and the interleave means 202 is configured to decide a data stream being an object of revising the data arrangement on the basis of the random number.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-72184
(P2004-72184A)
(43)公開日　平成16年3月4日(2004.3.4)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04L	9/32	H04L	9/00	675A	5C063
H04L	9/08	H04N	7/08	Z	5J104
H04L	9/14	H04L	9/00	601B	
H04N	7/08	H04L	9/00	641	
H04N	7/081				

審査請求 未請求　請求項の数 9　OL　（全 18 頁）

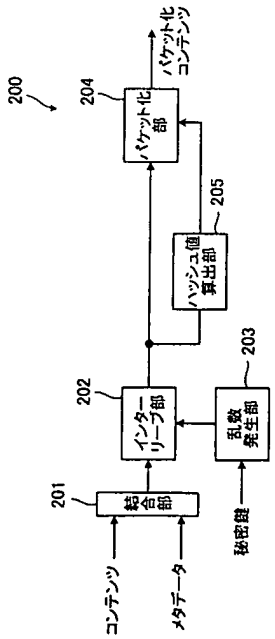
(21)出願番号　特願2002-225034(P2002-225034)
(22)出願日　平成14年8月1日(2002.8.1)

(71)出願人　000004352
日本放送協会
東京都渋谷区神南２丁目２番１号
(74)代理人　100072604
弁理士　有我　軍一郎
(72)発明者　小川　一人
東京都世田谷区砧一丁目１０番１１号　日本放送協会　放送技術研究所内
(72)発明者　合志　清一
東京都世田谷区砧一丁目１０番１１号　日本放送協会　放送技術研究所内
(72)発明者　室田　逸郎
東京都世田谷区砧一丁目１０番１１号　日本放送協会　放送技術研究所内

最終頁に続く

(54)【発明の名称】データ改竄防止装置およびそのプログラム

(57)【要約】
【課題】コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止装置およびそのプログラムを提供すること。
【解決手段】入力されるコンテンツとメタデータとを結合して結合データを生成する結合手段２０１と、秘密鍵を用いて乱数を発生する乱数発生手段２０３と、結合データ内のデータ配列を変更して配列入替データを生成するインターリーブ手段２０２と、配列入替データの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出手段２０５と、ハッシュ値に応じて配列入替データの所定部分のデータを変換してパケット化コンテンツを生成するパケット化手段２０４とを備え、インターリーブ手段２０２がデータ配列を変更する対象のデータ列を乱数に基づいて決定する構成を有している。
【選択図】　図２



【特許請求の範囲】
【請求項１】
入力されるコンテンツとメタデータとを結合して結合データを生成する結合手段と、前記結合データ内のデータ配列を変更して配列入替データを生成するインターリーブ手段と、前記配列入替データの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出手段と、前記ハッシュ値に応じて前記配列入替データの所定部分のデータを変換してパケット化コンテンツを生成するパケット化手段とを備えたことを特徴とするデータ改竄防止装置。
【請求項２】
入力されるメタデータの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出手段と、入力されたコンテンツの所定部分のデータを前記ハッシュ値に応じて変換して変換データを生成し前記変換データと前記メタデータと結合して結合変換データを生成するパケット化手段と、前記結合変換データ内のデータ配列を変更してパケット化コンテンツを生成するインターリーブ手段とを備えたことを特徴とするデータ改竄防止装置。
【請求項３】
前記データ改竄防止装置は、さらに秘密鍵を用いて乱数を発生する乱数発生手段を備え、前記インターリーブ手段は、前記データ配列を変更する対象のデータ列を前記乱数に基づいて決定することを特徴とする請求項１または請求項２記載のデータ改竄防止装置。
【請求項４】
請求項１記載のデータ改竄防止装置によって生成されたパケット化コンテンツに応じて前記データ改竄防止装置が算出するハッシュ値と同一のハッシュ値を算出するハッシュ値算出手段と、前記ハッシュ値に応じて前記パケット化コンテンツを逆変換して前記データ改竄防止装置が生成する前記配列入替データと同一の配列入替データに戻す逆パケット化手段と、前記配列入替データのデータ配列を変更して前記データ改竄防止装置が生成する結合データと同一の結合データに戻すインターリーブ手段と、前記結合データを前記コンテンツと前記メタデータとに分離するメタデータ分離手段とを備えたことを特徴とするデータ改竄防止装置。
【請求項５】
請求項２記載のデータ改竄防止装置によって生成されたパケット化コンテンツのデータ配列を変更して前記データ改竄防止装置が生成する結合変換データと同一の結合変換データに戻すインターリーブ手段と、前記結合変換データを前記データ改竄防止装置によって変換された変換データと前記メタデータとに分離するメタデータ分離手段と、前記メタデータに応じて前記データ改竄防止装置が算出するハッシュ値と同一のハッシュ値を算出するハッシュ値算出手段と、前記ハッシュ値に応じて前記データ改竄防止装置によって変換された変換データを逆変換して元のコンテンツを生成する逆パケット化手段とを備えたことを特徴とするデータ改竄防止装置。
【請求項６】
前記データ改竄防止装置は、さらに請求項１または請求項２記載のデータ改竄防止装置に入力される秘密鍵を用いて請求項１または請求項２記載のデータ改竄防止装置が発生する乱数と同一の乱数を発生する乱数発生手段を備え、前記インターリーブ手段は、前記乱数に基づいてデータ配列を元に戻す対象のデータ列を決定することを特徴とする請求項４または請求項５記載のデータ改竄防止装置。
【請求項７】
コンピュータに、入力されるコンテンツとメタデータとを結合して結合データを生成する結合ステップと、前記結合データ内のデータ配列を変更して配列入替データを生成するインターリーブステップと、前記配列入替データの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出ステップと、前記ハッシュ値に応じて前記配列入替データの所定部分のデータを変換してパケット化コンテンツを生成するパケット化ステップとを実行させることを特徴とするデータ改竄防止プログラム。
【請求項８】

コンピュータに、入力されるメタデータの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出ステップと、入力されたコンテンツの所定部分のデータを前記ハッシュ値に応じて変換して変換データを生成し前記変換データと前記メタデータと結合して結合変換データを生成するパケット化ステップと、前記結合変換データ内のデータ配列を変更してパケット化コンテンツを生成するインターリーブステップとを実行させることを特徴とするデータ改竄防止プログラム。

【請求項９】

前記データ改竄防止プログラムは、さらにコンピュータに、秘密鍵を用いて乱数を発生する乱数発生ステップを実行させ、前記インターリーブステップで、前記データ配列を変更する対象のデータ列を前記乱数に基づいて決定することを特徴とする請求項７または請求項８記載のデータ改竄防止プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンテンツの流通過程における、コンテンツの改竄またはコンテンツに付加されるメタデータ等の改竄を困難にするためのデータ改竄防止装置およびそのプログラムに関する。

【０００２】

【従来の技術】

従来、コンテンツの流通過程において、コンテンツにメタデータと呼ばれる付加情報を加えて配信する場合、コンテンツのヘッダとして、メタデータを付加し、一つのコンテンツパケットとして配信することが一般的であった。ここで、メタデータは、これが付加されたコンテンツに関するものであり、ヘッダ部分に組み込まれているため、コンテンツと容易に分離可能であり、改竄が容易であった。

【０００３】

そのため、コンテンツに対応するメタデータを容易に取得できないようにするために、コンテンツにメタデータを付加せず、コンテンツの配信とメタデータの配信のタイミングをずらすことや、コンテンツをパッケージにして配送してメタデータをネットワーク経由で配信する等の別系統でコンテンツとメタデータを届けること等が行われている。この場合も、メタデータとコンテンツとは一体ではなく、始めから分離されている。

【０００４】

また、コンテンツやメタデータの改竄防止のために、コンテンツやメタデータを暗号化してから配信することが一般に行われている。しかし、この場合も、コンテンツとメタデータは別々に暗号化され、容易に分離できるような構造となっていた。

【０００５】

【発明が解決しようとする課題】

しかしながら、従来の技術では、コンテンツとメタデータとは分離できるものであり暗号化されていても個別に解読することができるため、メタデータを不正に改竄することが容易であるという問題があった。その結果、メタデータとして、例えば、コンテンツの視聴制御情報、視聴回数制限情報、コピー回数制御情報等が含まれる場合に、これらを改竄し、制限回数を超えた視聴や、コピー制御を無効にしたコピーが可能となることがあっり、分離されたコンテンツのみが不正にコピーされるおそれがあった。

【０００６】

本発明は、かかる問題を解決するためになされたもので、その目的は、コンテンツとメタデータに分離困難な変換処理を施すことによって、コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止装置およびそのプログラムを提供することにある。

【０００７】

【課題を解決するための手段】

以上の点を考慮して、請求項１に係る発明は、入力されるコンテンツとメタデータとを結

合して結合データを生成する結合手段と、前記結合データ内のデータ配列を変更して配列入替データを生成するインターリーブ手段と、前記配列入替データの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出手段と、前記ハッシュ値に応じて前記配列入替データの所定部分のデータを変換してパケット化コンテンツを生成するパケット化手段とを備えた構成を有している。

【０００８】

この構成により、コンテンツとメタデータとを結合して一体としてから、データ配列を変更しデータを変換してパケット化コンテンツを生成するため、コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止装置を実現できる。

【０００９】

また、請求項２に係る発明は、入力されるメタデータの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出手段と、入力されたコンテンツの所定部分のデータを前記ハッシュ値に応じて変換して変換データを生成し前記変換データと前記メタデータと結合して結合変換データを生成するパケット化手段と、前記結合変換データ内のデータ配列を変更してパケット化コンテンツを生成するインターリーブ手段とを備えた構成を有している。

【００１０】

この構成により、コンテンツとメタデータとを結合して一体としてから、データ配列を変更しデータを変換してパケット化コンテンツを生成するため、コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止装置を実現できる。

【００１１】

また、請求項３に係る発明は、請求項１または請求項２において、前記データ改竄防止装置は、さらに秘密鍵を用いて乱数を発生する乱数発生手段を備え、前記インターリーブ手段は、前記データ配列を変更する対象のデータ列を前記乱数に基づいて決定する構成を有している。

【００１２】

この構成により、秘密鍵を用いて発生したハッシュ値を用いてデータ配列の変更を行っているため、データのわずかな改竄が行われた場合でも、ハッシュ値が大きく変化するため、コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止装置を実現できる。

【００１３】

また、請求項４に係る発明は、請求項１記載のデータ改竄防止装置によって生成されたパケット化コンテンツに応じて前記データ改竄防止装置が算出するハッシュ値と同一のハッシュ値を算出するハッシュ値算出手段と、前記ハッシュ値に応じて前記パケット化コンテンツを逆変換して前記データ改竄防止装置が生成する前記配列入替データと同一の配列入替データに戻す逆パケット化手段と、前記配列入替データのデータ配列を変更して前記データ改竄防止装置が生成する結合データと同一の結合データに戻すインターリーブ手段と、前記結合データを前記コンテンツと前記メタデータとに分離するメタデータ分離手段とを備えた構成を有している。

【００１４】

この構成により、コンテンツとメタデータとを結合して一体としてからパケット化されたコンテンツを逆変換によって再生するため、コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止装置を実現できる。

【００１５】

また、請求項５に係る発明は、請求項２記載のデータ改竄防止装置によって生成されたパケット化コンテンツのデータ配列を変更して前記データ改竄防止装置が生成する結合変換データと同一の結合変換データに戻すインターリーブ手段と、前記結合変換データを前記データ改竄防止装置によって変換された変換データと前記メタデータとに分離するメタデータ分離手段と、前記メタデータに応じて前記データ改竄防止装置が算出するハッシュ値と同一のハッシュ値を算出するハッシュ値算出手段と、前記ハッシュ値に応じて前記デー

タ改竄防止装置によって変換された変換データを逆変換して元のコンテンツを生成する逆パケット化手段とを備えた構成を有している。

【００１６】

この構成により、コンテンツとメタデータとを結合して一体としてからパケット化されたコンテンツを逆変換によって再生するため、コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止装置を実現できる。

【００１７】

また、請求項６に係る発明は、請求項４または請求項５において、前記データ改竄防止装置は、さらに請求項１または請求項２記載のデータ改竄防止装置に入力される秘密鍵を用いて請求項１または請求項２記載のデータ改竄防止装置が発生する乱数と同一の乱数を発生する乱数発生手段を備え、前記インターリーブ手段は、前記乱数に基づいてデータ配列を元に戻す対象のデータ列を決定する構成を有している。

【００１８】

この構成により、パケット化コンテンツの生成に用いられる秘密鍵と同一の秘密鍵を用いて発生した同一のハッシュ値を用いて逆変換するため、データのわずかな改竄が行われた場合でも、ハッシュ値が大きく変化し、コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止装置を実現できる。

【００１９】

また、請求項７に係る発明は、コンピュータに、入力されるコンテンツとメタデータとを結合して結合データを生成する結合ステップと、前記結合データ内のデータ配列を変更して配列入替データを生成するインターリーブステップと、前記配列入替データの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出ステップと、前記ハッシュ値に応じて前記配列入替データの所定部分のデータを変換してパケット化コンテンツを生成するパケット化ステップとを実行させる構成を有している。

【００２０】

この構成により、コンテンツとメタデータとを結合して一体としてから、データ配列を変更しデータを変換してパケット化コンテンツを生成するため、コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止プログラムを実現できる。

【００２１】

また、請求項８に係る発明は、コンピュータに、入力されるメタデータの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出ステップと、入力されたコンテンツの所定部分のデータを前記ハッシュ値に応じて変換して変換データを生成し前記変換データと前記メタデータと結合して結合変換データを生成するパケット化ステップと、前記結合変換データ内のデータ配列を変更してパケット化コンテンツを生成するインターリーブステップとを実行させる構成を有している。

【００２２】

この構成により、コンテンツとメタデータとを結合して一体としてから、データ配列を変更しデータを変換してパケット化コンテンツを生成するため、コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止プログラムを実現できる。

【００２３】

また、請求項９に係る発明は、請求項７または請求項８において　前記データ改竄防止プログラムは、さらにコンピュータに、秘密鍵を用いて乱数を発生する乱数発生ステップを実行させ、前記インターリーブステップで、前記データ配列を変更する対象のデータ列を前記乱数に基づいて決定する構成を有している。

【００２４】

この構成により、秘密鍵を用いて発生したハッシュ値を用いてデータ配列の変更を行っているため、データのわずかな改竄が行われた場合でも、ハッシュ値が大きく変化するため、コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止プログラムを実現できる。

【００２５】

【発明の実施の形態】
以下、本発明の実施の形態に係るデータ改竄防止装置およびそのプログラムについて、添付図面を用いて説明する。
（第１の実施の形態）
図１は、本発明の第１の実施形態に係るデータ改竄防止システム１００の構成を示すブロック図である。データ改竄防止システム１００は、プロバイダ側に構成されるシステムであり、ユーザ側のユーザ端末１１０からの要求をインターネット１２０を介して受信し、要求に応じたコンテンツとメタデータとをパケット化して配信するシステムである。
【００２６】
図１に示すデータ改竄防止システム１００では、制御中継装置１０１がユーザ端末１１０からインターネット１２０を介して送信されたコンテンツ配信要求を受信し、制御中継装置１０１の制御の下、コンテンツパケット化サーバ１０５が要求されたコンテンツをコンテンツサーバ１０３から、このコンテンツに付加するメタデータをメタデータサーバ１０４から、受け取ってパケット化されたコンテンツ（以下、単にパケット化コンテンツという。）を作成し、コンテンツ配信サーバ１０６がこのパケット化コンテンツをユーザ端末１１０に配信する。
【００２７】
制御中継装置１０１は、ユーザ端末１１０からインターネット１２０を介して送信されたコンテンツ配信要求を受信し、要求されたコンテンツに応じたパケット化コンテンツの生成から配送までの各処理を実行させるために各サーバの制御および中継処理を行うようになっている。
イントラネット１０２は、これに接続されるサーバ間のデータ通信を可能とするＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）等のネットワークである。
【００２８】
コンテンツサーバ１０３は、コンテンツを記憶しているサーバであり、ユーザ端末１１０によって要求されたコンテンツをコンテンツパケット化サーバ１０５に送信する。なお、コンテンツは暗号化されていても、暗号化されていなくてもよい。
メタデータサーバ１０４は、メタデータを記憶しているサーバであり、ユーザ端末１１０によって要求されたコンテンツに付加するメタデータをコンテンツパケット化サーバ１０５に送信する。なお、メタデータは暗号化されていても暗号化されていなくてもよい。
【００２９】
コンテンツパケット化サーバ１０５は、コンテンツサーバ１０３から送信されたコンテンツと、メタデータサーバ１０４から送信されたメタデータとを合成してパケット化コンテンツを生成する。
コンテンツ配信サーバ１０６は、コンテンツパケット化サーバ１０５が生成したパケット化コンテンツをコンテンツの配信を要求したユーザ端末１１０に制御中継装置１０１経由で配信する。
【００３０】
図２は、本発明の第１の実施形態に係るデータ改竄防止装置であるコンテンツパケット化サーバの構成を示すブロック図である。図２では、図１に示すコンテンツパケット化サーバ１０５をデータ改竄防止装置（コンテンツパケット化サーバ）２００として表す。データ改竄防止装置（コンテンツパケット化サーバ）２００は、入力されるコンテンツとメタデータとを結合して結合データを生成する結合部２０１、秘密鍵を用いて乱数を発生する乱数発生部２０３、結合データ内のデータ配列を変更して配列入替データを生成するインターリーブ部２０２、配列入替データの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出部２０５、およびハッシュ値に応じて配列入替データの所定部分のデータを変換してパケット化コンテンツを生成するパケット化部２０４を有する。
【００３１】
結合部２０１は、入力されたコンテンツおよびメタデータを結合して１つの結合データにするようになっている。

インターリーブ部２０２は、結合部２０１から出力されるビットの並びである結合データ内のデータ配列の順番を入れ替え、配列入替データを生成するようになっている。入れ替えにおいて乱数発生部２０３が発生した乱数に基づいて入れ替え位置を決定することができる。なお、乱数を用いずに予め決められた入れ替え位置のデータを入れ替えることもできるが、入替え位置を探知されることによって乱数を用いた場合よりも改竄の危険性が高い。

【００３２】

乱数発生部２０３は、乱数を発生するようになっている。乱数発生部２０３には、秘密鍵が入力され、秘密鍵を用いて乱数を発生するのでもよい。乱数の発生は秘密鍵に基づいて行われ、かかる技術は公知であるため、その説明を省略する。また、秘密鍵としては、任意の数値にするのでも良い。

【００３３】

パケット化部２０４は、インターリーブ部２０２によってデータ配列が入れ替えられて得られたデータである配列入替データが入力され、この配列入替データの所定位置のデータをハッシュ値算出部２０５から受け取ったハッシュ値に応じて変換してパケット化コンテンツを生成し、生成したパケット化コンテンツを外部に出力するようになっている。

【００３４】

ハッシュ値算出部２０５は、配列入替データ内の所定部分のデータに応じたハッシュ値を算出し、パケット化部２０４に出力するようになっている。ハッシュ値は、ハッシュ関数を用いて生成されるデータであり、ハッシュ値の算出技術は公知であるため説明を省略する。

【００３５】

以下、図３および図４を用いて本発明の第１の実施の形態に係るデータ改竄防止方法について説明する。

本発明の第１の実施の形態に係るデータ改竄防止方法では、入力されたコンテンツとメタデータとが結合部２０１によって結合されて一つの結合データが生成され（ステップＳ３０１）、入力された秘密鍵に応じて乱数が乱数発生部２０３によって発生され（ステップＳ３０２）、発生した乱数に基づいて結合データ内のデータ配列の入替えがインターリーブ部２０２によって行なわれ配列入替データが生成され（ステップＳ３０３）、配列入替データ４１０における予め決められた位置を占めるデータ４１１に応じてハッシュ値４２０が生成され（ステップＳ３０４）、データ４１１以外の所定のデータ４１２がデータ４１２とハッシュ値との演算により変換されパケット化コンテンツ４３０が生成される（ステップＳ３０５）。

【００３６】

以下に、パケット化コンテンツの生成（ステップＳ３０５）について、図４を用いて具体的に説明する。パケット化コンテンツ４３０の生成において、処理対象の入力データ（配列入替データ）は、その内の所定部分のデータがハッシュ値を用いて変換されるものである。ここで、図４に示すように配列入替データ４１０が構成され、ハッシュ値の算出に用いられるデータ４１１が「１０１１１１１・・・」であり、データ４１１に基づいて算出されたハッシュ値４２０が「００１０１１００」であり、変換対象のデータ列４１２の一例が「１１０００１１０」であるとする。

【００３７】

図４には、上記の演算として排他的論理和を適用した例が示されている。この例では、変換対象のデータ列４１２の一例である「１１０００１１０」とハッシュ値４２０である「００１０１１００」との排他的論理和の計算が行われて変換後のデータ列４３１「１１１０１０１０」が算出され、データ４１２に置き換えられてパケット化コンテンツ４３０内に配置される。

【００３８】

なお、上記の演算は、排他的論理和に限られず、可換な演算であればよい。また、ビット単位の演算でも複数ビットをまとめた演算であってもよい。ただし、変換対象のデータ列

４１２は、ハッシュ値の算出に用いられるデータ列以外の部分とする。コンテンツの再生を可能とするためである。

【００３９】

また、本発明の第１の実施の形態では、上記のステップＳ３０１からＳ３０５までの各ステップでの処理を行うデータ改竄防止方法について説明したが、これらのステップＳ３０１からＳ３０５までの各ステップでの処理を含むデータ改竄防止動作を実行させるためのデータ改竄防止プログラムを生成し、そのプログラムに基づいて、コンピュータに、これらのステップＳ３０１からＳ３０５までの各ステップでの処理を含むデータ改竄防止動作を実行させることも可能である。

【００４０】

以上説明したように、本発明の第１の実施の形態に係るデータ改竄防止装置およびプログラムは、コンテンツとメタデータとを結合して一体としてから、データ配列を変更しデータを変換してパケット化コンテンツを生成するため、コンテンツまたはメタデータの改竄を困難にすることができる。

また、秘密鍵を用いて発生したハッシュ値を用いてデータ配列の変更を行っているため、データのわずかな改竄が行われた場合でも、ハッシュ値が大きく変化するため、コンテンツまたはメタデータの改竄を困難にすることができる。

【００４１】

（第２の実施の形態）

図５は、本発明の第２の実施形態に係るデータ改竄防止装置の構成を示すブロック図である。図５に示すデータ改竄防止装置５００は、本発明の第１の実施の形態に係るデータ改竄防止システム１００にコンテンツの配信を要求するユーザ端末１１０に含まれ、データ改竄防止システムから送信されユーザ端末１１０が受信したパケット化コンテンツを再生するための装置である。

【００４２】

データ改竄防止装置５００は、本発明の第１の実施の形態に係るデータ改竄防止装置によって生成されたパケット化コンテンツに応じてデータ改竄防止装置が算出するハッシュ値と同一のハッシュ値を算出するハッシュ値算出部５０１、算出したハッシュ値に応じてパケット化コンテンツを逆変換して本発明の第１の実施の形態に係るデータ改竄防止装置が生成する配列入替データと同一の配列入替データに戻す逆パケット化部５０２、本発明の第１の実施の形態に係るデータ改竄防止装置に入力される秘密鍵を用いて、このデータ改竄防止装置が発生する乱数と同一の乱数を発生する乱数発生部５０４、配列入替データのデータ配列を変更して本発明の第１の実施の形態に係るデータ改竄防止装置が生成する結合データと同一の結合データに戻すインターリーブ部５０３、および復元された結合データをコンテンツとメタデータとに分離するメタデータ分離部５０５を有する。

【００４３】

ハッシュ値算出部５０１は、入力されたパケット化コンテンツの予め決められた位置に配置されたデータに応じたハッシュ値を算出するようになっている。上記の予め決められた位置としては、パケット化コンテンツの送信側でハッシュ値の算出に用いたデータが配置された位置として予め決められた位置をいい、ハッシュ値算出部５０１は、同一の送信側と同一のハッシュ値を算出するものである。

【００４４】

逆パケット化部５０２は、受信したパケット化コンテンツをハッシュ値算出部５０１が発生したハッシュ値を用いてパケット化を解いて元の配列入替データとするようになっている。これは、上記のパケット化の処理を逆方向に行うことによって実現される。なお、ハッシュ値を演算して得られたデータを元のデータに変換するには、同一のハッシュ値を用いた逆演算を行うことで実現できる。排他的論理和を例に取ると、逆演算も排他的論理和となる。

【００４５】

インターリーブ部５０３は、逆パケット化部５０２によってパケット化が解かれたデータ

である配列入替データ内のデータ配列の順番を元に戻し、元の結合データを生成するようになっている。元に戻す処理は、乱数発生部５０４が発生した乱数に基づいてデータが入れ替えられた位置を算出することによって実現できる。なお、乱数を発生させてデータの入れ替えを行っていない場合は、予め決められた位置のデータの配列を入れ替えるものとする。

【００４６】

乱数発生部５０４は、乱数を発生するようになっている。なお、データ改竄防止装置（コンテンツパケット化サーバ）２００の乱数発生部２０３が秘密鍵を用いる場合、乱数発生部５０４にも、これと同一の秘密鍵が入力され、秘密鍵を用いてデータ改竄防止装置（コンテンツパケット化サーバ）２００の乱数発生部２０３が発生する乱数と同一の乱数を発生する。

【００４７】

メタデータ分離部５０５は、インターリーブ部５０３によって生成された元の結合データからメタデータを分離し、コンテンツとメタデータとを別々に出力するようになっている。

以上の各構成部は、データ改竄防止装置（コンテンツパケット化サーバ）２００によって行われた処理の逆変換を行うものであり、逆変換によって元のコンテンツとメタデータを再生するものである。

【００４８】

以下、図６を用いて本発明の第２の実施の形態に係るデータ改竄防止方法について説明する。

本発明の第２の実施の形態に係るデータ改竄防止方法では、入力されたパケット化コンテンツの所定部分のデータに応じたハッシュ値がハッシュ値算出部５０１によって算出され（ステップＳ６０１）、パケット化コンテンツの予め決められた位置のデータが逆パケット化部５０２によってハッシュ値を用いて逆演算処理されてパケット化が解かれ（ステップＳ６０２）、パケット化が解かれたデータの配列を戻すためのデータが乱数発生部５０４によって発生され（ステップＳ６０３）、パケット化が解かれたデータがインターリーブ部５０３によって元のコンテンツ等のデータ配列に戻され（ステップＳ６０４）、元のコンテンツ等のデータ配列に変換されたデータからメタデータがメタデータ分離部５０５によって分離される（ステップＳ６０５）。

【００４９】

本発明の第２の実施の形態に係るデータ改竄防止装置およびそのプログラムでは、ハッシュ値とコンテンツ等との演算を行ってコンテンツ等を変換することにより、コンテンツの改竄に対する対策が行われている。ハッシュ値を求めるための、ＳＨＡ１のようなハッシュ関数は入力データ内のほんの小さな部分が変化しても、その出力値が大きく変化する関数である。このため、もし、メタデータに改竄が行われた場合、そのハッシュ値は大きく変化する。この大きく変化してしまったハッシュ値とパケット化されたコンテンツの演算を行い、もとのコンテンツを復元することは困難である。これにより、メタデータの改竄防止、コンテンツの改竄防止を行うことができる。

【００５０】

また、本発明の第２の実施の形態では、上記のステップＳ６０１からＳ６０５までの各ステップでの処理を行うデータ改竄防止方法について説明したが、これらのステップＳ６０１からＳ６０５までの各ステップでの処理を含むデータ改竄防止動作を実行させるためのデータ改竄防止プログラムを生成し、そのプログラムに基づいて、コンピュータに、これらのステップＳ６０１からＳ６０５までの各ステップでの処理を含むデータ改竄防止動作を実行させることも可能である。

【００５１】

以上説明したように、本発明の第２の実施の形態に係るデータ改竄防止装置およびプログラムは、コンテンツとメタデータとを結合して一体としてからパケット化されたコンテンツを逆変換によって再生するため、コンテンツまたはメタデータの改竄を困難にすること

ができる。

【００５２】

（第３の実施の形態）

図７は、本発明の第３の実施形態に係るデータ改竄防止装置であるコンテンツパケット化サーバの構成を示すブロック図である。図７では、図１に示すコンテンツパケット化サーバ１０５をデータ改竄防止装置（コンテンツパケット化サーバ）７００として表す。データ改竄防止装置（コンテンツパケット化サーバ）７００は、入力されるメタデータの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出部７０１、入力されたコンテンツの所定部分のデータをハッシュ値に応じて変換して変換データを生成し変換データとメタデータと結合して結合変換データを生成するパケット化部７０２、乱数を発生する乱数発生部７０４、および結合変換データ内のデータ配列を変更してパケット化コンテンツを生成するインターリーブ部７０３を有する。

【００５３】

ハッシュ値算出部７０１は、入力されたメタデータに応じたハッシュ値を算出し、パケット化部７０２に出力するようになっている。ハッシュ値の算出には、メタデータの一部を使用するのでも、全部を使用するのでも良い。

パケット化部７０２は、ハッシュ値算出部７０１からハッシュ値が入力され、このハッシュ値を用いてコンテンツ内の予め決められた部分のデータを変換して変換データを生成し、変換データとメタデータとを結合して結合変換データするようになっている。

【００５４】

この変換について図８を用いて説明する。図８に示すように入力コンテンツ８１０が与えられ、ハッシュ値８２０が「００１０１１００」と得られたとする。入力コンテンツ８１０の内、「１１０００１１０」の部分８１１を変換対象の部分とすると、変換は、例えば部分８１１「１１０００１１０」とハッシュ値８２０「００１０１１００」との排他的論理和をとることによって行われる。

【００５５】

なお、この演算についても上記の第１の実施の形態と同様に排他的論理和に限られず、可換な演算であれば他の演算であってもよい。また、コンテンツ内で、ハッシュ値を用いて変換する部分は予め定められたものであってもよいが、乱数を発生させ、発生した乱数に応じた部分を変換するようにしても良く、ビット単位の演算でも複数ビットまとめた演算であってもよい。

【００５６】

インターリーブ部７０３は、パケット化部７０２から出力された結合変換データ内のデータ配列の順番を入れ替えるようになっている。入れ替えにおいて乱数発生部７０４が発生した乱数に基づいて入れ替え位置を決定することができる。なお、乱数を用いずに予め決められた入れ替え位置のデータを入れ替えることもできるが、入替え位置を探知されることによって乱数を用いた場合よりも改竄の危険性が高い。

【００５７】

乱数発生部７０４は、乱数を発生し、発生した乱数をインターリーブ部７０３に出力するようになっている。乱数発生部７０４には、秘密鍵が入力され、秘密鍵を用いて乱数を発生するのでもよい。乱数の発生は秘密鍵に基づいて行われ、かかる技術は公知であるため、その説明を省略する。また、秘密鍵としては、任意の数値にするのでも良い。

以上の構成によりインターリーブ部７０３からはパケット化コンテンツが出力されるようになっている。

【００５８】

以下、図９を用いて本発明の第３の実施の形態に係るデータ改竄防止方法について説明する。

本発明の第３の実施の形態に係るデータ改竄防止方法では、入力されたメタデータに応じたハッシュ値がハッシュ値算出部７０１によって生成され（ステップＳ９０１）、入力されたコンテンツの所定部分がパケット化部７０２によってハッシュ値に応じて変換され（

ステップＳ９０２）、入力された秘密鍵に応じて乱数が乱数発生部７０４によって発生され（ステップＳ９０３）、発生した乱数に基づいて結合変換データ内のデータ列の入替えがインターリーブ部７０３によって行なわれパケット化コンテンツが生成される（ステップＳ９０４）。

【００５９】

また、本発明の第３の実施の形態では、上記のステップＳ９０１からＳ９０４までの各ステップでの処理を行うデータ改竄防止方法について説明したが、これらのステップＳ９０１からＳ９０４までの各ステップでの処理を含むデータ改竄防止動作を実行させるためのデータ改竄防止プログラムを生成し、そのプログラムに基づいて、コンピュータに、これらのステップＳ９０１からＳ９０４までの各ステップでの処理を含むデータ改竄防止動作を実行させることも可能である。

【００６０】

以上説明したように、本発明の第３の実施の形態に係るデータ改竄防止装置およびプログラムは、コンテンツとメタデータとを結合して一体としてから、データ配列を変更しデータを変換してパケット化コンテンツを生成するため、コンテンツまたはメタデータの改竄を困難にすることができる。

また、秘密鍵を用いて発生したハッシュ値を用いてデータ配列の変更を行っているため、データのわずかな改竄が行われた場合でも、ハッシュ値が大きく変化するため、コンテンツまたはメタデータの改竄を困難にすることができる。

【００６１】

（第４の実施の形態）

図１０は、本発明の第４の実施形態に係るデータ改竄防止装置の構成を示すブロック図である。図１０に示すデータ改竄防止装置１０００は、本発明の第３の実施の形態に係るデータ改竄防止システム１００にコンテンツの配信を要求するユーザ端末１１０に含まれ、本発明の第３の実施の形態に係るデータ改竄防止システムから送信されユーザ端末１１０が受信したパケット化コンテンツを再生するための装置である。

【００６２】

データ改竄防止装置１０００は、乱数を発生させる乱数発生部１００２、発生した乱数に基づいてパケット化コンテンツのデータ配列を元に戻すインターリーブ部１００１、インターリーブ部１００１から出力されたデータの内メタデータを分離するメタデータ分離部１００３、分離されたメタデータに応じたハッシュ値を算出するハッシュ値算出部１００４、およびメタデータ分離部１００３により分離され出力されたデータであってハッシュ値を用いて変換されたコンテンツを元のコンテンツに戻す逆パケット化部１００５を有する。

【００６３】

インターリーブ部１００１は、乱数発生部１００２が発生した乱数に基づいてパケット化コンテンツのデータ配列を元に戻すようになっている。元に戻す処理は、乱数発生部１００２が発生した乱数に基づいてデータが入れ替えられた位置を算出するものとする。なお、乱数を発生させてデータの入れ替えを行っていない場合は、予め決められた位置のデータの配列を入れ替えるものとする。

【００６４】

乱数発生部１００２は、乱数を発生するようになっている。なお、データ改竄防止装置（コンテンツパケット化サーバ）７００の乱数発生部７０４が秘密鍵を用いる場合、乱数発生部１００２にも、これと同一の秘密鍵が入力され、秘密鍵を用いてデータ改竄防止装置（コンテンツパケット化サーバ）７００の乱数発生部７０４が発生する乱数と同一の乱数を発生する。

【００６５】

メタデータ分離部１００３は、インターリーブ部１００１によって元のデータ配列に戻されたデータからメタデータを分離し、分離したメタデータはハッシュ値算出部１００４および外部に出力され、残りのデータ（以下、変換コンテンツという。）は、逆パケット化

部１００５に出力されるようになっている。

【００６６】

ハッシュ値算出部１００４は、メタデータ分離部１００３から入力されたメタデータの予め決められた位置に配置されたデータに応じたハッシュ値を算出するようになっている。上記の予め決められた位置としては、メタデータの送信側で上記のようにハッシュ値を算出したデータが配置された位置として予め決められた位置をいう。

【００６７】

逆パケット化部１００５は、メタデータ分離部１００３から入力された変換コンテンツをハッシュ値算出部１００４が発生したハッシュ値を用いて逆変換し、元のコンテンツとするようになっている。これは、本発明の第３の実施の形態のパケット化処理を逆方向に行うことによって実現される。なお、逆変換は、変換の際に生成したハッシュ値と同一のハッシュ値を用いて逆演算を行うことにより実現できる。排他的論理和を例に取ると、逆演算も排他的論理和となる。

【００６８】

以上の各構成部は、データ改竄防止装置（コンテンツパケット化サーバ）７００によって行われた処理の逆変換を行うものであり、逆変換によって元のコンテンツとメタデータを再生するものである。

【００６９】

以下、図１１を用いて本発明の第４の実施の形態に係るデータ改竄防止方法について説明する。

本発明の第４の実施の形態に係るデータ改竄防止方法では、本発明の第３の実施の形態に係るデータ改竄防止装置７００の乱数発生部７０４が用いる秘密鍵と同一の秘密鍵を用いて、同一の乱数が乱数発生部１００２によって発生され（ステップＳ１１０１）、ステップＳ１１０１で発生した乱数に基づいてパケット化コンテンツのデータ配列がインターリーブ部１００１によって元に戻され（ステップＳ１１０２）、ステップＳ１１０２で元のデータ配列に戻されたデータからメタデータがメタデータ分離部１００３によって分離されてメタデータと変換コンテンツが生成され（ステップＳ１１０３）、ステップＳ１１０３で生成されたメタデータの予め決められた位置に配置されたデータに応じたハッシュ値がハッシュ値算出部１００４によって算出され（ステップＳ１１０４）、ステップＳ１１０３で生成された変換コンテンツがステップＳ１１０４で発生したハッシュ値を用いて逆パケット化部１００５によって逆変換されて元のコンテンツに戻される（ステップＳ１１０５）。

【００７０】

本発明の第４の実施の形態に係るデータ改竄防止装置およびそのプログラムでは、ハッシュ値とコンテンツ等との演算を行ってコンテンツ等を変換することにより、コンテンツの改竄に対する対策が行われている。ハッシュ値を求めるための、ＳＨＡ１のようなハッシュ関数は入力データ内のほんの小さな部分が変化しても、その出力値が大きく変化する関数である。このため、もし、メタデータに改竄が行われた場合、そのハッシュ値は大きく変化する。この大きく変化してしまったハッシュ値とパケット化されたコンテンツの演算を行い、もとのコンテンツを復元することは不可能である。これにより、メタデータの改竄防止、コンテンツの改竄防止を行うことができる。

【００７１】

また、本発明の第４の実施の形態では、上記のステップＳ１１０１からＳ１１０５までの各ステップでの処理を行うデータ改竄防止方法について説明したが、これらのステップＳ１１０１からＳ１１０５までの各ステップでの処理を含むデータ改竄防止動作を実行させるためのデータ改竄防止プログラムを生成し、そのプログラムに基づいて、コンピュータに、これらのステップＳ１１０１からＳ１１０５までの各ステップでの処理を含むデータ改竄防止動作を実行させることも可能である。

【００７２】

以上説明したように、本発明の第４の実施の形態に係るデータ改竄防止装置およびプログ

ラムは、コンテンツとメタデータとを結合して一体としてからパケット化されたコンテンツを逆変換によって再生するため、コンテンツまたはメタデータの改竄を困難にすることができる。

【００７３】

【発明の効果】

以上説明したように、本発明は、コンテンツとメタデータに分離困難な変換処理を施すことによって、コンテンツまたはメタデータの改竄を防止することが可能なデータ改竄防止装置およびそのプログラムを提供することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係るデータ改竄防止システムの構成を示す図である。

【図２】本発明の第１の実施形態に係るデータ改竄防止装置の構成を示すブロック図である。

【図３】本発明の第１の実施形態に係るデータ改竄防止方法における処理の流れを示すフローチャートである。

【図４】本発明の第１の実施形態に係るデータ改竄防止方法の説明図である。

【図５】本発明の第２の実施形態に係るデータ改竄防止装置の構成を示すブロック図である。

【図６】本発明の第２の実施形態に係るデータ改竄防止方法における処理の流れを示すフローチャートである。

【図７】本発明の第３の実施形態に係るデータ改竄防止装置の構成を示すブロック図である。

【図８】本発明の第３の実施形態に係るデータ改竄防止装置における処理の説明図である。

【図９】本発明の第３の実施形態に係るデータ改竄防止方法における処理の流れを示すフローチャートである。

【図１０】本発明の第４の実施形態に係るデータ改竄防止装置の構成を示すブロック図である。

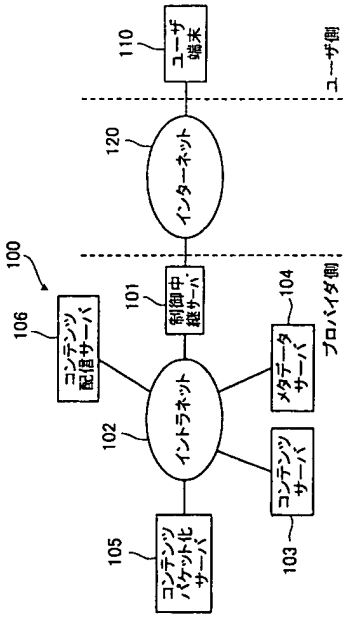
【図１１】本発明の第４の実施形態に係るデータ改竄防止方法における処理の流れを示すフローチャートである。

【符号の説明】

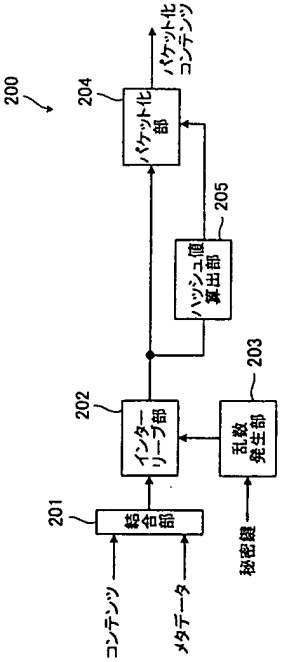
１００　データ改竄防止システム
１０１　制御中継装置
１０２　イントラネット
１０３　コンテンツサーバ
１０４　メタデータサーバ
１０５　コンテンツパケット化サーバ
１０６　コンテンツ配信サーバ
１１０　ユーザ端末
１２０　インターネット
２００、７００　データ改竄防止装置（コンテンツパケット化サーバ）
２０１　結合部
２０２、５０３、７０３、１００１　インターリーブ部
２０３、５０４、７０４、１００２　乱数発生部
２０４、７０２　パケット化部
２０５、５０１、７０１、１００４　ハッシュ値算出部
４１０　入力データ（配列入替データ）
４１１　ハッシュ値の算出に用いるデータ部分
４１２、８１１　演算対象のデータ列の一例
４２０、８２０　ハッシュ値
４３０、８３０　出力データ

４３１、８３１　変換後のデータ列
５００、１０００　データ改竄防止装置
５０２、１００５　逆パケット化部
５０５、１００３　メタデータ分離部
８１０　入力コンテンツ

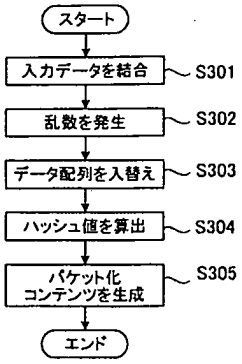
【図１】



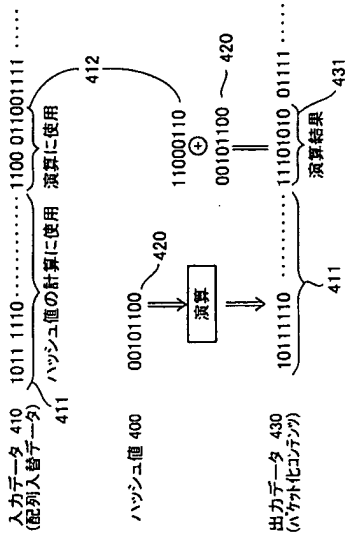
【図２】



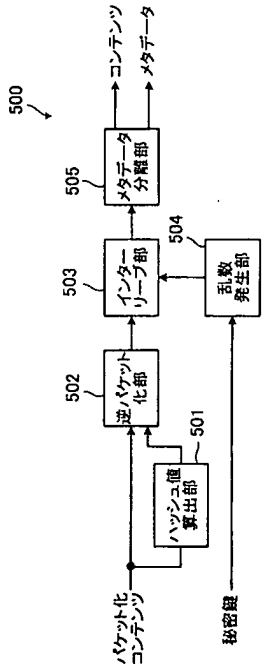
【図３】


スタート
入力データを結合
S301
乱数を発生
S302
データ配列を入替え
S303
ハッシュ値を算出
S304
パケット化
コンテンツを生成
S305
エンド

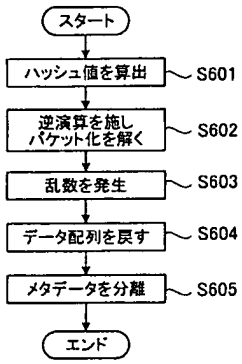
【図４】


入力データ 410
(配列入替データ)
411
1011 1110
ハッシュ値の計算に使用
1100 011001111
演算に使用
412
ハッシュ値 400
00101100
420
演算
11000110
00101100
出力データ 430
(パケット化コンテンツ)
10111110
411
11101010 01111
演算結果
431

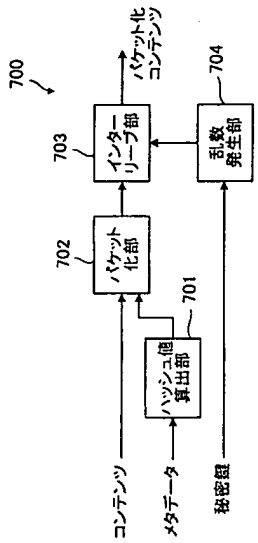
【図５】


500
コンテンツ
メタデータ
505
メタデータ分離部
503
インターリーブ部
504
乱数発生部
502
逆パケット化部
501
ハッシュ値算出部
パケット化コンテンツ
秘密鍵

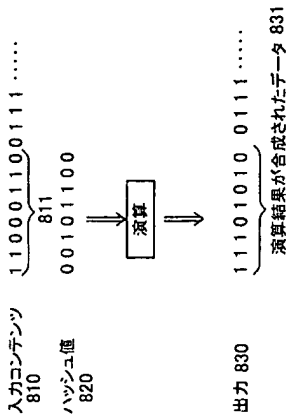
【図６】


スタート
ハッシュ値を算出
S601
逆演算を施し
パケット化を解く
S602
乱数を発生
S603
データ配列を戻す
S604
メタデータを分離
S605
エンド

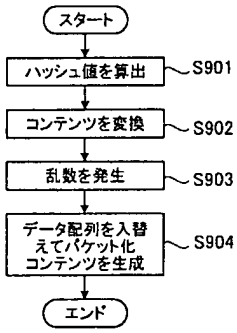
【図７】


700
パケット化コンテンツ
703
インターリーブ部
704
乱数発生部
702
パケット化部
701
ハッシュ値算出部
コンテンツ
メタデータ
秘密鍵

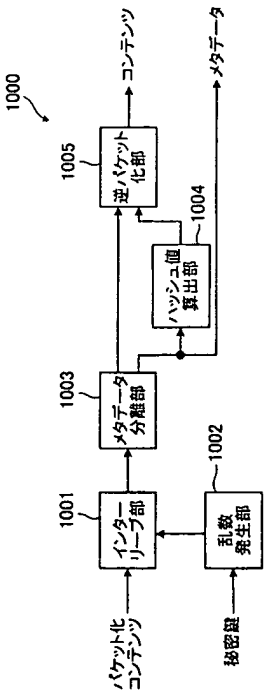
【図８】


入力コンテンツ 810
ハッシュ値 820
1100011001111……
811
00101100
演算
11101010 0111……
出力 830
演算結果が合成されたデータ 831

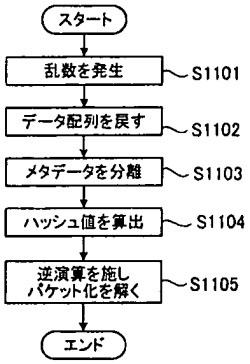
【図９】


スタート
ハッシュ値を算出
S901
コンテンツを変換
S902
乱数を発生
S903
データ配列を入替えてパケット化コンテンツを生成
S904
エンド

【図１０】


1000
コンテンツ
メタデータ
1005
逆パケット化部
1004
ハッシュ値算出部
1003
メタデータ分離部
1001
インターリーブ部
1002
乱数発生部
パケット化コンテンツ
秘密鍵

【図１１】


スタート
乱数を発生
S1101
データ配列を戻す
S1102
メタデータを分離
S1103
ハッシュ値を算出
S1104
逆演算を施し
パケット化を解く
S1105
エンド

フロントページの続き

(72)発明者 大竹 剛
東京都世田谷区砧一丁目１０番１１号 日本放送協会 放送技術研究所内

Ｆターム(参考) 5C063 AB03 AB05 AC01 AC10 CA23 DA07 DA13
5J104 AA08 AA13 JA01 JA03 LA01 LA02 LA05 NA09 NA10 NA12
PA14